

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB09-152

### Vulnerability Summary for the Week of May 25, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology ( NIST ) National Vulnerability Database ( NVD ) in the past week. The NVD is sponsored by the Department of Homeland Security ( DHS ) National Cyber Security Division ( NCSD ) / United States Computer Emergency Readiness Team ( US-CERT ). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) ( CVSS ) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities (CVSS Score: 7.0 .. 10.0)					
Primary Vendor -- Product	Description	Published	CVSS Score	Source Patch	
2daybiz -- custom_t-shirt_design_script	SQL injection vulnerability in product.php in 2daybiz Custom T-shirt Design Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-05-29	7.5	<a href="#">CVE-2009-1819</a> <a href="#">VUPEN-BID</a> <a href="#">MILWOF</a> <a href="#">SECUNIA</a>	
android -- android	The PackageManagerService class in services/java/com/android/server/PackageManagerService.java in Android 1.5 through 1.5 CRB42 does not properly check developer certificates during processing of sharedUserId requests at an application's installation time, which allows remote attackers to access application data by creating a package that specifies a shared user ID with an arbitrary application.	2009-05-26	7.5	<a href="#">CVE-2009-1754</a> <a href="#">MISC CONFIR</a>	
aten -- kh1516i_ip_kvm_switch aten -- kn9116_ip_kvm_switch	The Java client program for the ATEN KH1516i IP KVM switch with firmware 1.0.063 and the KN9116 IP KVM switch with firmware 1.1.104 has a hardcoded AES encryption key, which makes it easier for man-in-the-middle attackers to (1) execute arbitrary Java code, or (2) gain access to machines connected to the switch, by hijacking a session.	2009-05-27	10.0	<a href="#">CVE-2009-1472</a> <a href="#">BUGTRAQ</a>	
aten -- kh1516i_ip_kvm_switch aten -- kn9116_ip_kvm_switch	The (1) Windows and (2) Java client programs for the ATEN KH1516i IP KVM switch with firmware 1.0.063 and the KN9116 IP KVM switch with firmware 1.1.104 do not properly use RSA cryptography for a symmetric session-key negotiation, which makes it easier for remote attackers to (a) decrypt network traffic, or (b) conduct man-in-the-middle attacks, by repeating unspecified "client-side calculations."	2009-05-27	10.0	<a href="#">CVE-2009-1473</a> <a href="#">BUGTRAQ</a>	
	The ATEN KH1516i IP KVM switch with firmware 1.0.063 and the KN9116 IP KVM switch with firmware 1.1.104 do not (1)				

aten -- kh1516i_ip_kvm_switch aten -- kn9116_ip_kvm_switch	encrypt mouse events, which makes it easier for man-in-the-middle attackers to perform mouse operations on machines connected to the switch by injecting network traffic; and do not (2) set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2009-05-27	7.6	CVE-2009-1474 BUGTRAQ
aten -- kh1516i_ip_kvm_switch aten -- kn9116_ip_kvm_switch aten -- pn9108_power_over_the_net	The https web interfaces on the ATEN KH1516i IP KVM switch with firmware 1.0.063, the KN9116 IP KVM switch with firmware 1.1.104, and the PN9108 power-control unit have a hardcoded SSL private key, which makes it easier for remote attackers to decrypt https sessions by extracting this key from their own switch and then sniffing network traffic to a switch owned by a different customer.	2009-05-27	10.0	CVE-2009-1477 BUGTRAQ
avg -- avg_anti-virus	The AVG parsing engine 8.5.323, as used in multiple AVG anti-virus products including Anti-Virus Network Edition, Internet Security Netzwerk Edition, Server Edition für Linux/FreeBSD, Anti-Virus SBS Edition, and others allows remote attackers to bypass malware detection via a crafted (1) RAR and (2) ZIP archive.	2009-05-22	10.0	CVE-2009-1784 XF BID BUGTRAQ MISC
baofeng -- storm	Unspecified vulnerability in Config.dll in Baofeng products 3.09.04.17 and earlier allows remote attackers to execute arbitrary code by calling the SetAttributeValue method, as exploited in the wild in April and May 2009.	2009-05-28	9.3	CVE-2009-1807 MISC
chinagames -- igame	Stack-based buffer overflow in the Chinagames CGAgent ActiveX control 1.x in CGAgent.dll, as distributed in Chinagames iGame 2009, allows remote attackers to execute arbitrary code via a long argument to the CreateChinagames method, as exploited in the wild in April and May 2009. NOTE: some of these details are obtained from third party information.	2009-05-28	7.5	CVE-2009-1800 BID MISC SECUNI MISC MISC MISC
darren_reed -- ipfilter	Buffer overflow in lib/load_http.c in ippool in Darren Reed IPFilter (aka IP Filter) 4.1.31 allows local users to gain privileges via vectors involving a long hostname in a URL.	2009-05-26	7.2	CVE-2009-1476 BID SREASO CONFIR CONFIR
digimode10 -- maya	Multiple buffer overflows in DigiMode Maya 1.0.2 allow remote attackers to execute arbitrary code via a long string in a malformed (1) .m3u or (2) .m3l playlist file.	2009-05-29	9.3	CVE-2009-1817 XF BID MILWOf
eaton -- network_shutdown_module	Eaton MGEOPS Network Shutdown Module before 3.10 Build 13 allows remote attackers to execute arbitrary code by adding a custom action to the MGE frontend via pane_actionbutton.php, and then executing this action via exec_action.php.	2009-05-28	10.0	CVE-2009-6816 XF BID BUGTRAQ MISC SECUNI OSVDB CONFIR
f-prot -- f-prot_antivirus f-prot -- f-prot_aves f-prot -- f-prot_milter	Multiple FRISK Software F-Prot anti-virus products, including Antivirus for Exchange, Linux on IBM zSeries, Linux x86 File Servers, Linux x86 Mail Servers, Linux x86 Workstations, Solaris Mail Servers, Antivirus for Windows, and others, allow remote attackers to bypass malware detection via a crafted CAB archive.	2009-05-22	10.0	CVE-2009-1783 XF BID BUGTRAQ MISC
ibm -- hardware_management_console	Unspecified vulnerability in IBM Hardware Management Console (HMC) 7 release 3.4.0 SP2, when Active Memory Sharing is used, has unknown impact and attack vectors, related to a shared memory partition and a shared memory pool with redundant paging Virtual I/O Server (VIOS) partitions. NOTE: some of these details are obtained from third	2009-05-28	9.3	CVE-2009-1806 CONFIR

	party information.			
jevontech -- phpenpals	SQL injection vulnerability in mail.php in PHPenpals 1.1 and earlier allows remote attackers to execute arbitrary SQL commands via the ID parameter. NOTE: the profile.php vector is already covered by CVE-2006-0074.	2009-05-29	7.5	CVE-2009-1814 VUPEN BID MILWOf SECUNI
kernel -- linux linux -- kernel	Multiple buffer overflows in the cifs subsystem in the Linux kernel before 2.6.29.4 allow remote CIFS servers to cause a denial of service (memory corruption) and possibly have unspecified other impact via (1) a malformed Unicode string, related to Unicode string area alignment in fs/cifs/sess.c; or (2) long Unicode characters, related to fs/cifs/cifssmb.c and the cifs_readdir function in fs/cifs/readdir.c.	2009-05-28	7.8	CVE-2009-1633 FEDORA CONFIR MLIST MLIST MLIST CONFIR CONFIR CONFIR
maser_gonzalo -- com_artforms	Multiple PHP remote file inclusion vulnerabilities in the InterJoomla ArtForms (com_artforms) component 2.1b7 for Joomla! allow remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter to (1) imgcaptcha.php or (2) mp3captcha.php in assets/captcha/includes/captchaform/, or (3) assets/captcha/includes/captchatalog/swfmovie.php.	2009-05-29	7.5	CVE-2009-1822 BID MILWOf
maxcms -- maxcms	SQL injection vulnerability in admin/admin_manager.asp in MaxCMS 2.0 allows remote attackers to execute arbitrary SQL commands via an m_username cookie in an add action.	2009-05-29	7.5	CVE-2009-1818 XF VUPEN MILWOf
mega-nerd -- libsndfile nullsoft -- winamp	Heap-based buffer overflow in voc_read_header in libsndfile 1.0.15 through 1.0.19, as used in Winamp 5.552 and possibly other media programs, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a VOC file with an invalid header value.	2009-05-26	9.3	CVE-2009-1788 XF VUPEN VUPEN BID CONFIR CONFIR
mega-nerd -- libsndfile nullsoft -- winamp	Heap-based buffer overflow in aiff_read_header in libsndfile 1.0.15 through 1.0.19, as used in Winamp 5.552 and possibly other media programs, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via an AIFF file with an invalid header value.	2009-05-26	9.3	CVE-2009-1791 XF VUPEN BID CONFIR CONFIR
mygamescript -- mygamescript	SQL injection vulnerability in admin.php in My Game Script 2.0 allows remote attackers to execute arbitrary SQL commands via the user parameter (aka the username field). NOTE: some of these details are obtained from third party information.	2009-05-29	7.5	CVE-2009-1816 XF BID MILWOf SECUNI OSVDB
novell -- groupwise	The WebAccess component in Novell GroupWise 7.x before 7.03 HP3 and 8.x before 8.0 HP2 does not properly implement session management mechanisms, which allows remote attackers to gain access to user accounts via unspecified vectors.	2009-05-26	7.5	CVE-2009-1634 MISC VUPEN BID CONFIR SECUNI
	Multiple buffer overflows in the Internet Agent (aka GWIA)			CVE-2009-1636 MISC MISC MISC

novell -- groupwise	component in Novell GroupWise 7.x before 7.03 HP3 and 8.x before 8.0 HP2 allow remote attackers to execute arbitrary code via (1) a crafted e-mail address in an SMTP session or (2) an SMTP command.	2009-05-26	10.0	MISC VUPEN BID BID BUGTRA CONFIR CONFIR SECUNI
phpdirsubmit -- php_dir_submit	Multiple SQL injection vulnerabilities in PHP Dir Submit (aka WebsiteSubmitter and Submitter Script) allow remote attackers to bypass authentication and gain administrative access via the (1) username and (2) password parameters.	2009-05-26	7.5	CVE-2009-1787 BID MILWoF
pidgin -- pidgin	Buffer overflow in the XMPP SOCKS5 bytestream server in Pidgin before 2.5.6 allows remote authenticated users to execute arbitrary code via vectors involving an outbound XMPP file transfer. NOTE: some of these details are obtained from third party information.	2009-05-26	7.1	CVE-2009-1373 BID CONFIR
pidgin -- pidgin	Multiple integer overflows in the msn_slplink_process_msg functions in the MSN protocol handler in (1) libpurple/protocols/msn/slplink.c and (2) libpurple/protocols/msnp9/slplink.c in Pidgin before 2.5.6 on 32-bit platforms allow remote attackers to execute arbitrary code via a malformed SLP message with a crafted offset value, leading to buffer overflows. NOTE: this issue exists because of an incomplete fix for CVE-2008-2927.	2009-05-26	9.3	CVE-2009-1376 CONFIR
roboform -- frax.dk_php_recommend	admin.php in Frax.dk Php Recommend 1.3 and earlier does not require authentication when the user password is changed, which allows remote attackers to gain administrative privileges via modified form_admin_user and form_admin_pass parameters.	2009-05-22	7.5	CVE-2009-1780 VUPEN BID MILWoF
sonicspot -- audioactive_player	Stack-based buffer overflow in Sonic Spot Audioactive Player 1.93b allows remote attackers to execute arbitrary code via a long string in a playlist file, as demonstrated by a long .mp3 URL in a .m3u file.	2009-05-29	9.3	CVE-2009-1815 VUPEN BID MILWoF MILWoF
submitterscript -- submitterscript	Multiple SQL injection vulnerabilities in admin/index.php in Submitter Script 2 allow remote attackers to execute arbitrary SQL commands via (1) the uNev parameter (aka the username field) or (2) the uJelszo parameter (aka the Password field).	2009-05-29	7.5	CVE-2009-1813 XF VUPEN BID MILWoF SECUNI OSVDB
sun -- solaris	Heap-based buffer overflow in sadmind in Sun Solaris 8 and 9 allows remote attackers to execute arbitrary code via a crafted RPC request, related to improper decoding of request parameters.	2009-05-26	10.0	CVE-2009-3869 SUNALE CONFIR
sun -- solaris	Integer overflow in sadmind in Sun Solaris 8 and 9 allows remote attackers to execute arbitrary code via a crafted RPC request that triggers a heap-based buffer overflow, related to improper memory allocation.	2009-05-26	10.0	CVE-2009-3870 SUNALE CONFIR
surat_kabar -- phpwebnews	SQL injection vulnerability in bukutamu.php in phpWebNews 0.2 allows remote attackers to execute arbitrary SQL commands via the det parameter.	2009-05-22	7.5	CVE-2009-6812 XF BID MILWoF
videoscript -- youtube_video_script	Multiple SQL injection vulnerabilities in admin/index.php in VideoScript.us YouTube Video Script allow remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters.	2009-05-28	7.5	CVE-2009-1804 XF BID MILWoF

[Back to top](#)

Medium Vulnerabilities (CVSS Score: 4.0 .. 6.9)				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
.collector -- mycolex	Multiple cross-site scripting (XSS) vulnerabilities in myColex 1.4.2 allow remote attackers to inject arbitrary web script or HTML via (1) the year parameter to modules/kalender.php, (2) the Page parameter in a List action to modules/ereignis.php, (3) the Kontext parameter in a Search action to modules/kategorie.php, or (4) the image parameter to modules/image.php.	2009-05-29	4.3	CVE-2009-1809 BID MILWORM SECUNIA
.collector -- mycolex	Multiple SQL injection vulnerabilities in myColex 1.4.2 allow remote attackers to execute arbitrary SQL commands via (1) the formUser parameter (aka the Name field) to common/login.php, and allow remote authenticated users to execute arbitrary SQL commands via the ID parameter in a Detail action to (2) kategorie.php, (3) medium.php, (4) person.php, or (5) schlagwort.php in modules/, related to classes/class.perform.php.	2009-05-29	6.0	CVE-2009-1810 CONFIRM
.collector -- mygesuad	Multiple cross-site scripting (XSS) vulnerabilities in myGesuad 0.9.14 (aka 0.9) allow remote attackers to inject arbitrary web script or HTML via (1) the Page parameter in a List action to modules/ereignis.php, (2) the Kontext parameter in a Search action to modules/kategorie.php, (3) the image parameter to modules/image.php, or (4) the ID parameter in a Detail action to modules/sitzung.php.	2009-05-29	4.3	CVE-2009-1811 BID MILWORM SECUNIA
.collector -- mygesuad	Multiple SQL injection vulnerabilities in myGesuad 0.9.14 (aka 0.9) allow remote attackers to execute arbitrary SQL commands via (1) the formUser parameter (aka the Name field) to common/login.php, and allow remote authenticated users to execute arbitrary SQL commands via the ID parameter in a Detail action to (2) kategorie.php, (3) budget.php, (4) zahlung.php, or (5) adresse.php in modules/, related to classes/class.perform.php.	2009-05-29	6.0	CVE-2009-1812 CONFIRM
2daybiz -- custom_t-shirt_design_script	Cross-site scripting (XSS) vulnerability in product.php in 2daybiz Custom T-shirt Design Script allows remote attackers to inject arbitrary web script or HTML via the id parameter.	2009-05-29	4.3	CVE-2009-1820 VUPEN BID MILWORM
apache -- http_server	The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.	2009-05-28	4.9	CVE-2009-1195 CONFIRM CONFIRM
bigace -- bigace_cms	SQL injection vulnerability in the new user registration feature in BigACE CMS 2.5, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-05-22	6.8	CVE-2009-1778 CONFIRM CONFIRM
cgi_rescue -- rescue	Cross-site scripting (XSS) vulnerability in CGI RESCUE Trees before 2.11 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2009-05-26	4.3	CVE-2009-1790 BID
dmxready -- registration_manager	DMXReady Registration Manager 1.1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for databases/webblogmanager.mdb.	2009-05-29	5.0	CVE-2009-1821 VUPEN MILWORM
	mod/server.mod/servmsg.c in Eggheads Eggdrop and			

eggheads -- eggdrop eggheads -- eggdrop_irc_bot philip_moore -- windrop	Windrop 1.6.19 and earlier allows remote attackers to cause a denial of service (crash) via a crafted PRIVMSG that causes an empty string to trigger a negative string length copy. NOTE: this issue exists because of an incorrect fix for CVE-2007-2807.	2009-05-26	4.3	CVE-2009-1789 VUPEN CONFIRM
eyrie -- pam-krb5	pam_krb5 2.2.14 through 2.3.4, as used in Red Hat Enterprise Linux (RHEL) 5, generates different password prompts depending on whether the user account exists, which allows remote attackers to enumerate valid usernames.	2009-05-28	5.0	CVE-2009-1384 CONFIRM BID MLIST
f-secure -- anti-virus f-secure -- client_security f-secure -- home_server_security f-secure -- internet_gatekeeper f-secure -- internet_security f-secure -- linux_security	Multiple F-Secure anti-virus products, including Anti-Virus for Microsoft Exchange 7.10 and earlier; Internet Gatekeeper for Windows 6.61 and earlier, Windows 6.61 and earlier, and Linux 2.16 and earlier; Internet Security 2009 and earlier, Anti-Virus 2009 and earlier, Client Security 8.0 and earlier, and others; allow remote attackers to bypass malware detection via a crafted (1) ZIP and (2) RAR archive.	2009-05-22	6.8	CVE-2009-1782 CONFIRM
freepbx -- freepbx	Multiple cross-site scripting (XSS) vulnerabilities in FreePBX 2.5.1, and other 2.4.x, 2.5.x, and pre-release 2.6.x versions, allow remote attackers to inject arbitrary web script or HTML via the (1) display parameter to reports.php, the (2) order and (3) extdisplay parameters to config.php, and the (4) sort parameter to recordings/index.php. NOTE: some of these details are obtained from third party information.	2009-05-28	4.3	CVE-2009-1801 BID
freepbx -- freepbx	Multiple cross-site request forgery (CSRF) vulnerabilities in FreePBX 2.5.1, and other 2.4.x, 2.5.x, and pre-release 2.6.x versions, allow remote attackers to hijack the authentication of admins for requests that create a new admin account or have unspecified other impact.	2009-05-28	6.8	CVE-2009-1802 BID
freepbx -- freepbx	FreePBX 2.5.1, and other 2.4.x, 2.5.x, and pre-release 2.6.x versions, generates different error messages for a failed login attempt depending on whether the user account exists, which allows remote attackers to enumerate valid usernames.	2009-05-28	5.0	CVE-2009-1803 BID
ibm -- aix	The malloc subsystem in libc in IBM AIX 5.3 and 6.1 allows local users to create or overwrite arbitrary files via a symlink attack on the log file associated with the MALLOCDEBUG environment variable.	2009-05-26	6.9	CVE-2009-1786 SECTRACK CONFIRM
jan_de_graaff -- com_simpleboard	Unrestricted file upload vulnerability in image_upload.php in the SimpleBoard (com_simpleboard) component 1.0.1 and earlier for Mambo allows remote attackers to execute arbitrary code by uploading a file with an executable extension and an image/jpeg content type, then accessing this file via a direct request to the file in components/com_simpleboard/, a different vulnerability than CVE-2006-3528.	2009-05-28	6.8	CVE-2008-6814 XF BID MILWoRM
matt_wright -- formmail	CRLF injection vulnerability in FormMail.pl in Matt Wright FormMail 1.92, and possibly earlier, allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the redirect parameter.	2009-05-22	5.0	CVE-2009-1777 MISC BUGTRAQ SECUNIA
microsoft -- windows_xp	Microsoft Windows XP SP3 allows local users to cause a denial of service (system crash) by making an SPI_SETDESKWALLPAPER SystemParametersInfo call with an improperly terminated pvParam argument, followed by an SPI_GETDESKWALLPAPER SystemParametersInfo call.	2009-05-28	4.9	CVE-2009-1808 BID MISC
myktools -- myktools	mykdownload.php in MyKtools 2.4 does not require administrative authentication, which allows remote attackers to read a database backup by making a direct request, and then sending an unspecified request to the	2009-05-28	5.0	CVE-2008-6815 XF BID

	download page for the backup.			MILWoRM
lnetlabs -- nsd	Off-by-one error in the packet_read_query_section function in packet.c in nsd 3.2.1, and process_query_section in query.c in nsd 2.3.7, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors that trigger a buffer overflow.	2009-05-22	5.0	CVE-2009-1755 CONFIRM CONFIRM CONFIRM
novell -- groupwise	Multiple cross-site scripting (XSS) vulnerabilities in the WebAccess component in Novell GroupWise 7.x before 7.03 HP3 and 8.x before 8.0 HP2 allow remote attackers to inject arbitrary web script or HTML via (1) the User.lang parameter to the login page (aka gw/webacc), (2) style expressions in a message that contains an HTML file, or (3) vectors associated with incorrect protection mechanisms against scripting.	2009-05-22	4.3	CVE-2009-1635 CONFIRM
novell -- groupwise	Multiple cross-site scripting (XSS) vulnerabilities in the WebAccess login page (aka gw/webacc) in Novell GroupWise 7.x before 7.03 HP2 allow remote attackers to inject arbitrary web script or HTML via the (1) GWAP.version or (2) User.Theme (aka User.Theme.index) parameter.	2009-05-22	4.3	CVE-2009-1762 CONFIRM
pidgin -- pidgin	Buffer overflow in the decrypt_out function in Pidgin before 2.5.6 allows remote attackers to cause a denial of service (application crash) via a QQ packet.	2009-05-26	5.0	CVE-2009-1374 BID CONFIRM
pidgin -- pidgin	The PurpleCircBuffer implementation in Pidgin before 2.5.6 does not properly maintain a certain buffer, which allows remote attackers to cause a denial of service (memory corruption and application crash) via vectors involving the (1) XMPP or (2) Sametime protocol.	2009-05-26	5.0	CVE-2009-1375 BID CONFIRM
redhat -- certificate_system redhat -- dogtag_certificate_system	agent/request/op.cgi in the Registration Authority (RA) component in Red Hat Certificate System (RHCS) 7.3 and Dogtag Certificate System allows remote authenticated users to approve certificate requests queued for arbitrary agent groups via a modified request ID field.	2009-05-27	6.5	CVE-2009-0588 CONFIRM REDHAT
roboform -- frax.dk_php_recommend	Static code injection vulnerability in admin.php in Frax.dk Php Recommend 1.3 and earlier allows remote attackers to inject arbitrary PHP code into phpre_config.php via the form_aula parameter.	2009-05-22	6.8	CVE-2009-1781 VUPEN BID MILWoRM
sebastian-thiele -- st-gallery	Multiple SQL injection vulnerabilities in the getGalleryImage function in st_admin/gallery_output.php in ST-Gallery 0.1 alpha, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) gallery_category or (2) gallery_show parameter to example.php.	2009-05-28	6.8	CVE-2009-1799 XF BID MILWoRM BUGTRAQ
sun -- java_system_portal_server	Cross-site scripting (XSS) vulnerability in Sun Java System Portal Server 6.3.1, 7.1, and 7.2 allows remote attackers to inject arbitrary web script or HTML via vectors related to an error page.	2009-05-26	4.3	CVE-2009-1796 BID SUNALERT CONFIRM

[Back to top](#)**Low Vulnerabilities (CVSS Score: 0.0 .. 3.9)**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
drupal -- print	Cross-site scripting (XSS) vulnerability in the Print (aka Printer, e-mail and PDF versions) module 5.x before 5.x-4.7 and 6.x before 6.x-1.7, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML by modifying a document head, before the Content-Type  META element, to contain crafted UTF-8 byte sequences	2009-05-29	2.6	CVE-2009-1823 VUPEN CONFIRM

	that are treated as UTF-7 by Internet Explorer 6 and 7, a related issue to CVE-2009-1575.			
simone_rota -- slim_simple_login_manager	SLiM Simple Login Manager 1.3.0 places the X authority magic cookie (mcookie) on the command line when invoking xauth from (1) app.cpp and (2) switchuser.cpp, which allows local users to access the X session by listing the process and its arguments.	2009-05-22	2.1	<a href="#">CVE-2009-1756</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MLIST</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a> <a href="#">CONFIRM</a>

[Back to top](#)**Last updated June 01, 2009** Print This Document